Company Sensitive Data Policy

Employee Data

- **Employee ID**: Unique identifier for employees; sharing can expose personal records and violate GDPR.
- **Salary details**: Financial data; revealing it could lead to privacy issues, internal conflicts, or legal violations.
- **Health / medical records**: Protected under HIPAA/GDPR; sharing violates privacy laws and could harm employees.
- **Performance evaluations**: Confidential HR data; exposing it could create unfair treatment or legal liability.
- **Home addresses / personal phone numbers**: Personally identifiable information; sharing risks employee safety and privacy.

Intellectual Property

- **Source code for proprietary products**: Reveals company's trade secrets; unauthorized access can cause competitive harm.
- **Upcoming product designs (Project X)**: Confidential R&D plans; leaking can cause business loss or reputational damage.
- **Internal R&D strategies**: Strategic plans for company growth; sharing can be exploited by competitors.

Customer Data

- **Customer names, addresses, emails**: PII; violates GDPR/CCPA if exposed and risks company trust.
- **Credit card or billing info**: Highly sensitive financial information; leakage can lead to fraud or legal liability.
- **Transaction history / support tickets**: Confidential business info; exposure can affect client trust and violate contracts.

Company Data

- **Internal financial reports**: Proprietary financial data; exposure could affect stock prices or give competitors an advantage.

- **Vendor contracts**: Legal documents containing sensitive clauses; sharing can breach confidentiality agreements.